

# Hierarchical Multi-stage Gaussian Signaling Games<sup>★</sup>

Muhammed Ömer Sayın, Emrah Akyol, and Tamer Başar

*Coordinated Science Laboratory,  
University of Illinois at Urbana-Champaign,  
Urbana, IL 61801 USA*

---

## Abstract

We analyze in this paper finite horizon hierarchical signaling games between informed senders and decision maker receivers in a dynamic environment. The underlying information evolves in time while sender and receiver interact repeatedly. Different from the classical communication models, however, the sender and the receiver have different objectives and there is a hierarchy between the players such that the sender leads the game by announcing his policies beforehand. He needs to anticipate the reaction of the receiver and the impact of the actions on the horizon while controlling the transparency of the disclosed information at each interaction. With quadratic objective functions and stationary multi-variate Gaussian processes, evolving according to first order auto-regressive models, we show that memoryless linear sender policies are optimal (in the sense of game-theoretic hierarchical equilibrium) within the general class of policies.

*Key words:* Stackelberg games; Hierarchical decision making; Communications; Gaussian processes.

---

## 1 Introduction

In the era of smart devices, we have various systems having enhanced processing and efficient communication capabilities. Even though information exchange is generally useful in cooperative multi-agent networks, where each agent has the same goal, such as in the consensus networks [12], diversification in smart systems brings about inevitable mismatches in the objectives of different agents. This then leads to non-cooperative game formulations for smart systems in the disclosure of information [1, 2, 5, 17]. As an example, a trajectory controller can drive a tracking system to a desired path, different from the tracker's actual intent, by controlling the disclosed information [16].

To this end, consider the scenario of a sender (S) having access to some information and a receiver (R) needing this information to be able to take a particular action, impacting both S and R. In the classical communication setting, S seeks to transmit this information in the best possible way, leading to a full cooperation between him and R, toward mitigating the channel's impact on the transmitted signals. However, even if there exists an ideal (perfect) channel between S and R, if their objectives differ, absolute transparency of

the disclosed information is not a reasonable action for S in general [1, 2, 5, 17]. In a hierarchical game, also known as Stackelberg game, [3], R reacts after S's disclosure of information. Therefore, in the strategic settings, where objectives differ, S develops strategies<sup>1</sup> to control the transparency of the disclosed information.

Recently, the strategic information transmission in hierarchical signaling games has attracted substantial interest in various disciplines, including control theory [6, 16], information theory [1, 2], and economics [7, 17]. In [6], the authors study strategic sensor networks for Gaussian parameters and myopic quadratic objective functions, i.e., the players develop strategies just for the current stage irrespective of the horizon, by restricting the receiver strategies to affine functions. Reference [16] addresses the optimality of linear sender strategies within the general class of policies for myopic quadratic objectives. Reference [2] shows that linear sender strategies achieve the equilibrium within general class of policies even with additive Gaussian noise channels. In [17], the author demonstrates the optimality of linear sender strategies also for the multivariate Gaussian information and quadratic cost functions. In [7], the authors address the optimality of full or no disclosure for general information parameters.

In addition to the mismatched objectives in a communica-

---

<sup>★</sup> This paper was not presented at any IFAC meeting. Corresponding author M. Ö. Sayın. Tel. +1-217-898-5476.

*Email addresses:* sayin2@illinois.edu (Muhammed Ömer Sayın), akyol@illinois.edu (Emrah Akyol), basar1@illinois.edu (Tamer Başar).

---

<sup>1</sup> In this paper, we use the terms “policy” and “strategy” interchangeably.

tion system, the signaling game setting can also be considered as a dynamic deception game [8, 9, 13], where a player aims to deceive the other player, say victim, such that the victim's perception about an underlying phenomenon and correspondingly the victim's reaction is controlled in a desirable way. Hence, this approach brings about new security and resilience applications for cyber-physical systems that are vulnerable to cyber attacks, e.g., power grids, transportation systems, and cloud networks [10, 11, 18]. In particular, turning the problem around, it is possible to develop new dynamic cyber-security strategies aiming to deceive attackers through this novel approach.

Now, coming to this paper, we obtain here equilibrium achieving sender strategies in hierarchical signaling games with finite horizon. We show that memoryless linear sender strategies can yield multi-stage equilibrium with finite horizon for general quadratic objective functions and multivariate stationary Gaussian processes evolving according to first order auto-regressive models. Since sender strategies are linear-in-parameter, the corresponding equilibrium achieving receiver strategies are also linear. In particular, this extends the result for the optimality of linear strategies shown in [17] to the dynamic setting. We point out that in the dynamic setting, in addition to the mismatches between the objectives, the sender should also control the transparency of the disclosed information due to impact of the actions on future stages. At each stage, S faces a trade-off in terms of the current stage and all other future stages of the game while controlling the transparency of the disclosed information, and should develop strategies in a comprehensive manner over the horizon. We point out that reference [15] addresses, in a two-stage setting, the purity of sender strategies (whether policies should include irrelevant information or not) by restricting the sender policies to affine functions, but does not completely solve the problem. However, here we show that pure linear strategies achieve the equilibrium within the general class of policies.

We can list the main features of this paper as follows:

- We study dynamic hierarchical Gaussian signaling games with finite horizon for general quadratic objective functions.
- We show the existence of equilibrium achieving policies within the general class of strategies.
- We show that linear sender and receiver policies can yield the equilibrium for arbitrary (finitely many) number of stages.

The paper is organized as follows: In Section 2, we provide the problem description. In Section 3, we introduce and discuss the Stackelberg equilibrium. We provide a bounding optimization problem in Section 4 and show that this bound is achievable through linear sender strategies in Section 5. We conclude the paper in Section 6 with several remarks. An appendix provides proof for a technical result.

**Notations:**  $\mathbb{N}(0, \cdot)$  denotes the multivariate Gaussian distribution

with zero mean and designated covariance. We denote random variables by bold lower case letters, e.g.,  $\mathbf{x}$ . For a vector  $x$ ,  $x'$  denotes its transpose and  $\|x\|$  denotes its Euclidean ( $L^2$ ) norm. For a matrix  $A$ ,  $\text{tr}\{A\}$  denotes its trace. We denote the identity and zero matrices with the associated dimensions by  $I$  and  $O$ , respectively. For positive semi-definite matrices  $A$  and  $B$ ,  $A \succeq B$  means that  $A - B$  is also a positive semi-definite matrix.

## 2 Problem Description

Consider the two discrete-time, stationary, exogenous processes  $\{\mathbf{x}_k\}$ , the state, and  $\{\boldsymbol{\theta}_k\}$ , the bias, that evolve according to the following first-order autoregressive models

$$\begin{aligned}\mathbf{x}_{k+1} &= A_x \mathbf{x}_k + \mathbf{w}_k, \\ \boldsymbol{\theta}_{k+1} &= A_\theta \boldsymbol{\theta}_k + \mathbf{v}_k, \quad k = 1, 2, \dots,\end{aligned}$$

where  $A_x \in \mathbb{R}^{p \times p}$ ,  $A_\theta \in \mathbb{R}^{r \times r}$ ,  $\mathbf{x}_1 \sim \mathbb{N}(0, \Sigma_x)$ ,  $\boldsymbol{\theta}_1 \sim \mathbb{N}(0, \Sigma_\theta)$ , and  $\mathbf{x}_1$  is independent of  $\boldsymbol{\theta}_1$ . The additive noise processes  $\{\mathbf{w}_k\}$  and  $\{\mathbf{v}_k\}$  are white Gaussian vector processes, i.e.,  $\mathbf{w}_k \sim \mathbb{N}(0, \Sigma_w)$  and  $\mathbf{v}_k \sim \mathbb{N}(0, \Sigma_v)$ , which are independent of each other, and of the initial state  $\mathbf{x}_1$  and initial bias  $\boldsymbol{\theta}_1$ . We assume that the covariance matrices  $\Sigma_x$ ,  $\Sigma_\theta$ ,  $\Sigma_w$ , and  $\Sigma_v$  are all positive definite matrices.

Let there be two agents: a sender (S) and a receiver (R) who take actions under different objectives. Only S has access to the state and the bias variables. On the other side, R uses the disclosed information to make a decision according to his/her own objective, which is different from S's objective and does not depend on the bias parameters. However, even if the objectives of S and R are different, R's decision impacts both objectives. In that asymmetric information paradigm, we seek to formulate the players' best actions in certain equilibrium scenarios.

In particular, at time instant  $k$ , S has access to the realizations of  $\mathbf{x}_{[1,k]} := \mathbf{x}_1, \dots, \mathbf{x}_k$ , and  $\boldsymbol{\theta}_{[1,k]} := \boldsymbol{\theta}_1, \dots, \boldsymbol{\theta}_k$ ; which are denoted by  $x_{[1,k]} := x_1, \dots, x_n$ , and  $\theta_{[1,k]} := \theta_1, \dots, \theta_n$ , respectively. S's actions  $\mathbf{y}_k$ , for  $k = 1, \dots, n$ , are given by  $\mathbf{y}_k = \eta_k(\mathbf{x}_{[1,k]}, \boldsymbol{\theta}_{[1,k]})$ , where  $\eta_k : \mathbb{R}^{kp} \times \mathbb{R}^{kr} \rightarrow \mathbb{R}^{p+r}$  is a deterministic disclosure policy such that the following conditional probability is 1:

$$\mathbb{P}(\mathbf{y}_k = \mathbf{y}_k | \mathbf{x}_{[1,k]} = x_{[1,k]}, \boldsymbol{\theta}_{[1,k]} = \theta_{[1,k]}) = 1$$

for every  $x_j \in \mathbb{R}^p$  and  $\theta_j \in \mathbb{R}^r$ ,  $j = 1, \dots, k$ , and  $y_k = \eta_k(x_{[1,k]}, \theta_{[1,k]})$ . Particularly, S chooses the policy  $\eta_k(\cdot, \cdot)$  from the policy space  $\Omega_k$ , which is the set of all Lebesgue measurable functions from  $\mathbb{R}^{kp} \times \mathbb{R}^{kr}$  to  $\mathbb{R}^{p+r}$ .

Note that the codomain of the policies in  $\Omega_k$  is  $\mathbb{R}^{p+r}$ . However,  $\Omega_k$  is also a superset of the sets of all Lebesgue measurable functions from  $\mathbb{R}^{kp} \times \mathbb{R}^{kr}$  to  $\mathbb{R}^t$ , where  $t \leq p + r$ , i.e., any such strategy is also in  $\Omega_k$ . We principally set the codomain in such a way that S can choose full information

disclosure, i.e.,  $y_k = [x'_k \theta'_k]'$ , as in the classical information transmission when agents have a common goal.

R does not have access to the realizations of the state and bias parameters. However, he/she has access to the actions of S and takes actions  $\mathbf{u}_k$  that are given by  $\mathbf{u}_k = \gamma_k(\mathbf{y}_{[1,k]})$ , where  $\mathbf{y}_{[1,k]} := \mathbf{y}_1, \dots, \mathbf{y}_k$  and  $\gamma_k : \mathbb{R}^{k(p+r)} \rightarrow \mathbb{R}^m$  is a deterministic decision policy such that  $\mathbb{P}(\mathbf{u}_k = \gamma_k(\mathbf{y}_{[1,k]})) = 1$ , where  $\mathbf{y}_{[1,k]} := y_1, \dots, y_k$ , for every  $y_j \in \mathbb{R}^p$ ,  $j = 1, \dots, k$ , and  $\mathbf{u}_k = \gamma_k(\mathbf{y}_{[1,k]})$ . R chooses policy  $\gamma_k(\cdot)$  from the policy space  $\Gamma_k$ , which is the set of all Lebesgue measurable functions from  $\mathbb{R}^{k(p+r)}$  to  $\mathbb{R}^m$ , i.e.,  $\gamma_k \in \Gamma_k$ .

S and R construct the policies  $\eta_k$  and  $\gamma_k$ , respectively, according to their own objectives, both of which depend on R's actions. S wants to minimize the following quadratic finite horizon objective

$$J_T(\eta_{[1,n]}; \gamma_{[1,n]}) = \sum_{k=1}^n \mathbb{E} \{ \|B_x \mathbf{x}_k + B_\theta \boldsymbol{\theta}_k + B_u \mathbf{u}_k\|^2 \}, \quad (1)$$

where  $\eta_{[1,n]} := \eta_1, \dots, \eta_n$  and  $\gamma_{[1,n]} := \gamma_1, \dots, \gamma_n$ , over  $\eta_k(\cdot, \cdot) \in \Omega_k$  for  $k = 1, \dots, n$ , where  $B_x \in \mathbb{R}^{p \times p}$ ,  $B_\theta \in \mathbb{R}^{p \times r}$ , and  $B_u \in \mathbb{R}^{p \times m}$  are deterministic combination matrices with associated dimensions. R's objective does not match with S's objective (1) and R aims to minimize

$$J_R(\eta_{[1,n]}; \gamma_{[1,n]}) = \sum_{k=1}^n \mathbb{E} \{ \|C_x \mathbf{x}_k + C_u \mathbf{u}_k\|^2 \} \quad (2)$$

over  $\gamma_k(\cdot) \in \Gamma_k$  for  $k = 1, \dots, n$ , where  $C_x \in \mathbb{R}^{p \times p}$  and  $C_u \in \mathbb{R}^{p \times m}$ . We assume that the objective function (2) is strictly convex in receiver actions  $\mathbf{u}_{[1,k]}$ , so that  $\forall k \in \{1, \dots, n\}$  and for any given  $x_j \in \mathbb{R}^p$ ,  $j = 1, \dots, n$ , the set:

$$\left\{ \mathbf{u}_k^* \in \mathbb{R}^m \mid \mathbf{u}_k^* = \arg \min_{\mathbf{u}_k \in \mathbb{R}^m} \sum_{j=1}^n \|C_x x_j + C_u \mathbf{u}_j\|^2 \right\}$$

is a singleton. As an example, for  $p = m$  and  $C_x = C_u = I$ , (2) is a strictly convex function of receiver actions.

### 3 Stackelberg Equilibrium

In our setting, there is a hierarchy between the agents in the announcement of the policies such that S leads the game by announcing and sticking to his/her policies beforehand. Then, R reacts accordingly. However, even if S had an incentive to take another action based on that reaction of R, the corresponding R action would have also changed respectively due to the hierarchy. Therefore, S anticipates this and takes the appropriate action from the beginning. We can model such a scheme as a Stackelberg game between the players [3] such that the leader, i.e., S, chooses his policy based on the corresponding best response of the follower, i.e., R.

Due to the hierarchy, given the realizations of S's actions, i.e.,  $y_{[1,k]}$ , R makes a decision  $\mathbf{u}_k$  according to Bayes' rule. This reaction  $\mathbf{u}_k$  not only depends on the realizations of the actions, e.g.,  $y_k$ , but also the associated policies  $\eta_k(\cdot, \cdot)$ . Therefore in this Stackelberg game, we denote R's policies by  $\mathbf{u}_k = \gamma_k(\mathbf{y}_{[1,k]}; \eta_{[1,k]})$  instead of  $\gamma_k(\mathbf{y}_{[1,k]})$  in order to explicitly show the dependence on S's policies. Then, for each  $n$ -tuple of policies  $\eta_k \in \Omega_k$ ,  $k = 1, \dots, n$ , we let  $R_R(\eta_{[1,n]})$  be the reaction set of R. For finite-horizon objectives, we have

$$R_R(\eta_{[1,n]}) := \arg \min_{\substack{\gamma_k \in \Gamma_k, \\ k=1, \dots, n}} J_R(\eta_{[1,n]}; \gamma_{[1,n]}).$$

By the assumption that (2) is strictly convex in R's actions, the reaction set  $R_R$  is singleton, which implies that the corresponding best response policies of R, i.e., the posterior believes according to Bayes' rule, are unique. We denote this best response by  $\gamma_k^*(y_{[1,k]}; \eta_{[1,k]}) \in R_R$ .

Furthermore, there is a linear relation between the best R policies  $\gamma_k^*(\cdot)$  and the conditional expectation of the state  $\mathbf{x}_k$ . By (2), R's best stage- $k$  policy is given by

$$\gamma_k^* = \arg \min_{\gamma_k \in \Gamma_k} \mathbb{E} \{ \|C_x \mathbf{x}_k + C_u \gamma_k(\mathbf{y}_{[1,k]}; \eta_{[1,k]})\|^2 \}$$

and the minimizer is given by

$$\gamma_k^*(\mathbf{y}_{[1,k]}) = -(C_u' C_u)^{-1} C_u' C_x \hat{\mathbf{x}}_k,$$

almost everywhere. Corresponding to the best reactions of R, S seeks policies  $\eta_k^*$  which minimize  $J_T$  over  $\eta_k \in \Omega_k$ . Particularly, the optimization problem faced by S is given by

$$\min_{\substack{\eta_k \in \Omega_k, \\ k=1, \dots, n}} J_T(\eta_{[1,n]}; \gamma_1^*(y_1; \eta_1), \dots, \gamma_n^*(y_{[1,n]}; \eta_{[1,n]})). \quad (3)$$

We note that also in [14], the authors study dynamic cheap talk and signaling games with quadratic cost functions for a scalar state and a commonly known bias parameter. Therefore, different from our scheme, in [14] the non-cooperative Stackelberg game turns into a team problem such that sender and receiver end up having the same objectives.

### 4 A Lower Bound

For the quadratic objective functions (1) and (2), the optimization problem (3) faced by S can be written as

$$\min_{\substack{\eta_k \in \Omega_k, \\ k=1, \dots, n}} \sum_{k=1}^n \mathbb{E} \{ \|B_x \mathbf{x}_k + B_\theta \boldsymbol{\theta}_k - B_u (C_u' C_u)^{-1} C_u' C_x \hat{\mathbf{x}}_k\|^2 \}. \quad (4)$$

Note that (4) is a quadratic function of  $\mathbf{x}_k$ ,  $\boldsymbol{\theta}_k$ , and  $\hat{\mathbf{x}}_k$  and in the following, we show that the objective function (4) can be written in terms of the second moment of posteriors

of the state and the bias given S's actions. To this end, let  $\mathbf{s}_k := [\mathbf{x}'_k \ \boldsymbol{\theta}'_k]'$  and  $\hat{\mathbf{s}}_k := [\hat{\mathbf{x}}'_k \ \hat{\boldsymbol{\theta}}'_k]'$  so that

$$\begin{aligned} & \mathbb{E}\{\|B_x \mathbf{x}_k + B_\theta \boldsymbol{\theta}_k - B_u (C'_u C_u)^{-1} C'_u C_x \hat{\mathbf{x}}_k\|^2\} \\ &= \mathbb{E}\left\{\| [B_x \ B_\theta] \mathbf{s}_k - [C \ O] \hat{\mathbf{s}}_k \|^2\right\} \\ &= \mathbb{E}\left\{\mathbf{s}'_k \begin{bmatrix} B'_x B_x & B'_x B_\theta \\ B'_\theta B_x & B'_\theta B_\theta \end{bmatrix} \mathbf{s}_k\right\} - 2\mathbb{E}\left\{\hat{\mathbf{s}}'_k \begin{bmatrix} C' B_x & C' B_\theta \\ O & O \end{bmatrix} \mathbf{s}_k\right\} \\ &\quad + \mathbb{E}\left\{\hat{\mathbf{s}}'_k \begin{bmatrix} C' C & O \\ O & O \end{bmatrix} \hat{\mathbf{s}}_k\right\}, \end{aligned} \quad (5)$$

where  $C := B_u (C'_u C_u)^{-1} C'_u C_x$ . The first term on the right hand side of (5) is independent of  $\hat{\mathbf{s}}_k$ . For the second term, we have

$$\begin{aligned} \mathbb{E}\{\hat{\mathbf{s}}'_k \Delta \mathbf{s}_k\} &\stackrel{(a)}{=} \mathbb{E}\{\mathbb{E}\{\hat{\mathbf{s}}'_k \Delta \mathbf{s}_k | \mathbf{y}_{[1,k]}\}\} \\ &\stackrel{(b)}{=} \mathbb{E}\{\hat{\mathbf{s}}'_k \Delta \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k]}\}\} \\ &\stackrel{(c)}{=} \mathbb{E}\{\hat{\mathbf{s}}'_k \Delta \hat{\mathbf{s}}_k\}, \end{aligned} \quad (6)$$

where  $\Delta$  is an arbitrary deterministic matrix with associated dimensions. The equality (a) is due to the law of iterated expectations; (b) holds because  $\hat{\mathbf{s}}_k$  is a bounded function of  $\mathbf{y}_{[1,k]}$  almost everywhere, and given  $\mathbf{y}_{[1,k]}$ ,  $\hat{\mathbf{s}}_k$  is a deterministic parameter; and (c) is due to  $\hat{\mathbf{s}}_k = \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k]}\}$ . Therefore, we obtain

$$\begin{aligned} 2\mathbb{E}\left\{\hat{\mathbf{s}}'_k \begin{bmatrix} C' B_x & C' B_\theta \\ O & O \end{bmatrix} \mathbf{s}_k\right\} &= 2\mathbb{E}\left\{\hat{\mathbf{s}}'_k \begin{bmatrix} C' B_x & C' B_\theta \\ O & O \end{bmatrix} \hat{\mathbf{s}}_k\right\} \\ &= \mathbb{E}\left\{\hat{\mathbf{s}}'_k \begin{bmatrix} C' B_x + B'_x C & C' B_\theta \\ B'_\theta C & O \end{bmatrix} \hat{\mathbf{s}}_k\right\}. \end{aligned} \quad (7)$$

Then, substituting (7) in (5), we can re-write the optimization problem (4) as

$$\min_{\eta_k \in \Omega_k, k=1, \dots, n} \sum_{k=1}^n \mathbb{E}\{\hat{\mathbf{s}}'_k V \hat{\mathbf{s}}_k\}, \quad (8)$$

where  $V := \begin{bmatrix} C' C - C' B_x - B'_x C & -C' B_\theta \\ -B'_\theta C & 0 \end{bmatrix}$ .

We point out that in Reference [17], the author addresses multi-dimensional information disclosure for the single-stage case. To this end, he constructs a Semi-Definite Programming (SDP) problem as a bound on sender's objective function (named utility function in [17]) and shows that linear strategies for Gaussian parameters achieve this bound. Here, we employ a similar approach to extend these results to the dynamic setting by addressing the question of whether the linear strategies are still optimal within the general class of policies or not.

The first moments of the posteriors of the state and the bias  $\hat{\mathbf{s}}_k = \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k]}\}$  are zero since  $\mathbb{E}\{\hat{\mathbf{s}}_k\} = \mathbb{E}\{\mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k]}\}\} = \mathbb{E}\{\mathbf{s}_k\}$  by the law of iterated expectations, and

$$\mathbb{E}\{\mathbf{s}_k\} = [\mathbb{E}\{\mathbf{x}_k\}' \ \mathbb{E}\{\boldsymbol{\theta}_k\}']' = 0$$

is a zero-vector with dimension  $p + r$ . We define the covariance matrix of  $\hat{\mathbf{s}}_k$ , namely the posterior covariance, as  $R_k := \mathbb{E}\{(\hat{\mathbf{s}}_k - \mathbb{E}\{\hat{\mathbf{s}}_k\})(\hat{\mathbf{s}}_k - \mathbb{E}\{\hat{\mathbf{s}}_k\})'\} = \mathbb{E}\{\hat{\mathbf{s}}_k \hat{\mathbf{s}}_k'\}$ , and let  $\Sigma := \begin{bmatrix} \Sigma_x & \\ & \Sigma_\theta \end{bmatrix}$ , and  $A := \begin{bmatrix} A_x & \\ & A_\theta \end{bmatrix}$ .

We note that for multivariate Gaussian variables, the mean is well defined, which implies  $\hat{\mathbf{x}}_k$  and  $\hat{\boldsymbol{\theta}}_k$  exist by the Radon-Nikodym theorem. Furthermore, being multivariate Gaussian, the state and bias parameters are integrable, i.e.,  $\mathbb{E}\{|\mathbf{x}_k|\}, \mathbb{E}\{|\boldsymbol{\theta}_k|\} < \infty$ , hence  $\hat{\mathbf{x}}_k$  and  $\hat{\boldsymbol{\theta}}_k$  are finite almost surely, which implies that  $\mathbb{E}\{\hat{\mathbf{x}}_k \hat{\mathbf{x}}_k'\}, \mathbb{E}\{\hat{\mathbf{x}}_k \hat{\boldsymbol{\theta}}_k'\}, \mathbb{E}\{\hat{\boldsymbol{\theta}}_k \hat{\boldsymbol{\theta}}_k'\}$  also exist.

Using these new parameters,  $R_k$ ,  $\Sigma$ , and  $A$ , the following lemma provides a lower bound for the minimization problem in (8).

**Lemma 1** *There exists a semi-definite programming (SDP) problem bounding the minimization problem (8) from below and given by<sup>2</sup>*

$$\begin{aligned} & \min_{\substack{S_k \in \mathbb{S}^{p+r}, \\ k=1, \dots, n}} \sum_{k=1}^n \text{tr}\{V S_k\} \\ & \text{s.t. } \Sigma \succeq S_1 \succeq O, \\ & \quad \Sigma \succeq S_j \succeq A S_{j-1} A', \ j = 2, \dots, n. \end{aligned} \quad (9)$$

**PROOF.** The minimization problem in (8) can be written as

$$\min_{\eta_k \in \Omega_k, k=1, \dots, n} \sum_{k=1}^n \text{tr}\{V \mathbb{E}\{\hat{\mathbf{s}}_k \hat{\mathbf{s}}_k'\}\} = \min_{\eta_k \in \Omega_k, k=1, \dots, n} \sum_{k=1}^n \text{tr}\{V R_k\}$$

since  $\text{tr}\{MN\} = \text{tr}\{NM\}$  for any matrices  $M$  and  $N$  if the multiplications are well posed, and  $\mathbb{E}\{\cdot\}$  is a linear operator. Note that the posterior covariances  $R_1, \dots, R_n$  depend on the policies  $\eta_1, \dots, \eta_n$ , and they are real and symmetric matrices by definition. The auto-covariance matrix  $\mathbb{E}\{(\mathbf{s}_k - \hat{\mathbf{s}}_k)(\mathbf{s}_k - \hat{\mathbf{s}}_k)'\} \succeq O$  can be written as

$$\begin{aligned} \mathbb{E}\{(\mathbf{s}_k - \hat{\mathbf{s}}_k)(\mathbf{s}_k - \hat{\mathbf{s}}_k)'\} &= \mathbb{E}\{\mathbf{s}_k \mathbf{s}_k'\} - \mathbb{E}\{\hat{\mathbf{s}}_k \mathbf{s}_k'\} - \mathbb{E}\{\mathbf{s}_k \hat{\mathbf{s}}_k'\} \\ &\quad + \mathbb{E}\{\hat{\mathbf{s}}_k \hat{\mathbf{s}}_k'\} \\ &= \Sigma - R_k, \end{aligned} \quad (10)$$

where  $\mathbb{E}\{\hat{\mathbf{s}}_k \mathbf{s}_k'\} = \mathbb{E}\{\mathbf{s}_k \hat{\mathbf{s}}_k'\} = \mathbb{E}\{\hat{\mathbf{s}}_k \hat{\mathbf{s}}_k'\}$  by (6). Therefore, we have  $\Sigma - R_k \succeq O$  and correspondingly  $\Sigma \succeq R_k$ , for  $k = 1, \dots, n$ . For the full information disclosure, e.g.,  $\eta_k(\mathbf{x}_{[1,k]}, \boldsymbol{\theta}_{[1,k]}) = [\mathbf{x}'_k \ \boldsymbol{\theta}'_k]'$ , we obtain  $\hat{\mathbf{s}}_k = \mathbf{s}_k$  and correspondingly  $R_k = \Sigma$ .

By construction, the posterior covariances  $R_k \succeq O$  are positive semi-definite matrices. For no information disclosure at stage-1, e.g.,  $\eta_1(\mathbf{x}_1, \boldsymbol{\theta}_1) = [0' \ 0']'$ , we obtain  $S_1 = O$ .

<sup>2</sup>  $\mathbb{S}^t$  denote the set of symmetric  $t \times t$  matrices.



However, even if  $S$  does not disclose any information at other stages, i.e.,  $k > 1$ , the posterior covariance  $S_k$ , for  $k = 2, \dots, n$ , may not be a zero matrix since  $R$ 's decision  $\gamma_k^*(y_{[1,k]}; \eta_{[1,k]})$  depends also on the previous stage strategies  $\eta_{[1,k-1]}$ . Correspondingly, if no information is disclosed at stage  $k > 1$ , i.e.,  $\eta_k = [0' \ 0']'$ , we obtain

$$\begin{aligned}\hat{\mathbf{s}}_{k,o} &= \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\} \\ &= \mathbb{E}\{A\mathbf{s}_{k-1} + \mathbf{z}_{k-1} | \mathbf{y}_{[1,k-1]}\} \\ &= A\hat{\mathbf{s}}_{k-1},\end{aligned}\quad (11)$$

where for clarity the subscript 'o' in  $\hat{\mathbf{s}}_{k,o}$  refers explicitly to no information being disclosed at stage- $k$ ,  $\mathbf{z}_j := [\mathbf{w}'_j \ \mathbf{v}'_j]'$ , for  $j = 1, \dots, n$ , is the noise vector, and  $\mathbb{E}\{A\mathbf{s}_{k-1} + \mathbf{z}_{k-1} | \mathbf{y}_{[1,k-1]}\} = A\mathbb{E}\{\mathbf{s}_{k-1} | \mathbf{y}_{[1,k-1]}\} = A\hat{\mathbf{s}}_1$  since  $\mathbf{z}_{k-1}$  and  $\mathbf{y}_1, \dots, \mathbf{y}_{k-1}$  are independent, and  $\mathbb{E}\{\mathbf{z}_{k-1}\} = \mathbf{0}$ . Then, we obtain  $R_{k,o} := \mathbb{E}\{\hat{\mathbf{s}}_{k,o} \hat{\mathbf{s}}_{k,o}'\} = \mathbb{E}\{A\hat{\mathbf{s}}_{k-1} \hat{\mathbf{s}}_{k-1}' A'\} = AS_{k-1}A'$ .

Next, we show that for any disclosure strategy at stage  $k > 1$ ,  $R_k \succeq AR_{k-1}A'$ . To this end, for an arbitrary disclosure policy  $\eta_k(\cdot, \cdot)$ , consider the positive semi-definite matrix:

$$\begin{aligned}& \mathbb{E}\{(\hat{\mathbf{s}}_k - \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\})(\hat{\mathbf{s}}_k - \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\})'\} \\ &= \mathbb{E}\{\hat{\mathbf{s}}_k \hat{\mathbf{s}}_k'\} + \mathbb{E}\{\mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\} \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\}'\} \\ &\quad - \mathbb{E}\{\hat{\mathbf{s}}_k \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\}'\} - \mathbb{E}\{\mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\} \hat{\mathbf{s}}_k'\},\end{aligned}\quad (12)$$

where the first and the second terms on the right hand side are given by  $R_k$  and  $R_{k,o} = AR_{k-1}A'$ , respectively. For the third term, we have

$$\begin{aligned}& \mathbb{E}\{\hat{\mathbf{s}}_k \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\}'\} \\ &= \mathbb{E}\{\mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\} \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\}'\} \\ &\stackrel{(a)}{=} \mathbb{E}\left\{\mathbb{E}\left\{\mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\} \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\}' \middle| \mathbf{y}_{[1,k-1]}\right\}\right\} \\ &\stackrel{(b)}{=} \mathbb{E}\left\{\mathbb{E}\left\{\mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\} \middle| \mathbf{y}_{[1,k-1]}\right\} \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\}'\right\} \\ &\stackrel{(c)}{=} \mathbb{E}\{\mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\} \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\}'\}, \\ &= AS_{k-1}A',\end{aligned}\quad (13)$$

where (a) is due to the law of iterated expectations; (b) holds because  $\mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\}$  is a bounded function of  $\mathbf{y}_{[1,k-1]}$  almost everywhere, and  $\mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\}$  is a deterministic parameter given  $\mathbf{y}_{[1,k-1]}$ ; and (c) is due to the iterated expectations with nested conditioning sets, i.e.,  $\{\mathbf{y}_{[1,k-1]}\} \subseteq \{\mathbf{y}_{[1,k]}\}$ . Note that the fourth term is the transpose of the third term. Substituting (13) in (12), we obtain

$$\begin{aligned}& \mathbb{E}\{(\hat{\mathbf{s}}_k - \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\})(\hat{\mathbf{s}}_k - \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k-1]}\})'\} \\ &= R_k - AR_{k-1}A',\end{aligned}$$

and therefore  $R_k - AR_{k-1}A' \succeq O$  and correspondingly  $R_k \succeq AR_{k-1}A'$ .

Ultimately, the posterior covariances  $R_1, \dots, R_k$  are real, symmetric matrices and should at least satisfy the constraints:  $\Sigma \succeq R_1 \succeq O$ , and  $\Sigma \succeq R_k \succeq AR_{k-1}A'$ , for  $k = 2, \dots, n$ . Based on this, we formulate another optimization problem (9) in which the optimization arguments  $S_1, \dots, S_n \in \mathbb{S}^{p+r}$  are subject to the constraints in (9). Since we have shown that those constraints are necessary (not necessarily sufficient yet), the minimization problem (9) is a lower bound on (8). Note that by the linear objective function  $\sum_k \text{tr}\{VS_k\}$  and the semi-definiteness constraints on  $S_k$ , (9) is an SDP problem.  $\square$

The following proposition addresses the existence of a solution for the SDP problem (9).

**Proposition 2** *The SDP problem (9) attains a global minimum.*

**PROOF.** We point out that by being a linear function, (9) is also a continuous function of the optimization arguments. And the constraint set is non-empty, e.g.,  $S_k = \Sigma$  for  $k = 1, \dots, n$  satisfies all constraints in (9). If we can show that the constraint set is compact over  $\mathbb{S}^{p+r} \times \dots \times \mathbb{S}^{p+r}$ , then the extreme value theorem implies that (9) attains a global minimum. To this end, for each  $k = 1, \dots, n$  and given  $S_{k-1}$  (set  $S_0 = O$ ), we define

$$\begin{aligned}\Psi_k(S_{k-1}) &:= \{S_k \in \mathbb{S}^{p+r} \mid \Sigma \succeq S_k \succeq AS_{k-1}A'\}, \\ \underline{\Psi}_k(S_{k-1}) &:= \{S_k \in \mathbb{S}^{p+r} \mid S_k \succeq AS_{k-1}A'\}, \text{ and} \\ \overline{\Psi}_k(S_{k-1}) &:= \{S_k \in \mathbb{S}^{p+r} \mid \Sigma \succeq S_k\}\end{aligned}$$

such that  $\Psi_k(S_{k-1}) = \underline{\Psi}_k(S_{k-1}) \cap \overline{\Psi}_k(S_{k-1})$ .

Let  $\mathbb{S}_+^{p+r}$  be the set of all positive semi-definite matrices with dimensions  $(p+r) \times (p+r)$  and consider the continuous mappings  $\underline{h}_k, \overline{h}_k : \mathbb{S}^{p+r} \rightarrow \mathbb{S}^{p+r}$  such that  $\underline{h}_k(S_k) = S_k - AS_{k-1}A'$  and  $\overline{h}_k(S_k) = \Sigma - S_k$ . Then, the constraint sets  $\underline{\Psi}_k(S_{k-1})$  and  $\overline{\Psi}_k(S_{k-1})$  are the pre-images of  $\mathbb{S}_+^{p+r}$  through the mappings  $\underline{h}_k$  and  $\overline{h}_k$ , respectively, i.e.,  $\underline{\Psi}_k(S_{k-1}) = \underline{h}_k^{-1}(\mathbb{S}_+^{p+r})$  and  $\overline{\Psi}_k(S_{k-1}) = \overline{h}_k^{-1}(\mathbb{S}_+^{p+r})$ . Since  $\mathbb{S}_+^{p+r}$  is a closed set over  $\mathbb{S}^{p+r}$ , the pre-images  $\underline{\Psi}_k(S_{k-1})$  and  $\overline{\Psi}_k(S_{k-1})$  are closed sets over  $\mathbb{S}^{p+r}$ . Then, their intersection  $\Psi_k(S_{k-1})$  is also a closed set.

Note that for any  $S_k \in \Psi_k(S_{k-1})$ , we have  $\mu'S_k\mu \leq \mu'\Sigma\mu \ \forall \ \mu \in \mathbb{R}^{p+r}$ , and therefore

$$\sup_{\|\mu\|=1} \mu'S_k\mu \leq \sup_{\|\mu\|=1} \mu'\Sigma\mu,$$

which implies that, since  $S_k, \Sigma \in \mathbb{S}^{p+r}$  are symmetric matrices, the spectral radius  $\rho(S_k) = \|S_k\|_2 \leq \rho(\Sigma)$  is bounded. Hence,  $\Psi_k(S_{k-1})$  is a closed and bounded set over  $\mathbb{S}^{p+r}$ .

Eventually, the constraint set as a cartesian product of the closed and bounded sets:

$$\Psi := \left\{ (S_1, \dots, S_n) \in \mathbb{S}^{p+r} \times \dots \times \mathbb{S}^{p+r} \mid \bigwedge_k S_k \in \Psi_k(S_{k-1}) \right\}$$

is closed and bounded. Since the underlying linear space  $\mathbb{S}^{p+r} \times \dots \times \mathbb{S}^{p+r}$  is finite dimensional, the constraint set  $\Psi \subset \mathbb{S}^{p+r} \times \dots \times \mathbb{S}^{p+r}$  is compact. Then, by invoking the extreme value theorem, we conclude that (9) attains a global minimum.  $\square$

The following theorem formulates the solution of (9) for an arbitrary (but finite) number of stages.

**Theorem 3** *For the  $n$ -stage problem, there exist symmetric idempotent matrices  $P_j \in \mathbb{S}^{p+r}$ , for  $j = 1, \dots, n$ , such that*

$$S_k^* = AS_{k-1}^*A' + (\Sigma - AS_{k-1}^*A')^{1/2}P_k(\Sigma - AS_{k-1}^*A')^{1/2}, \quad (14)$$

for  $k = 1, \dots, n$  (set  $S_0^* = O$ ), attains the global minimum of (9).

**PROOF.** We first point out that the constraint set in (9) is convex. To show this, consider  $n$ -tuples of symmetric matrices  $(M_1, \dots, M_n) \in \mathbb{S}^{p+r} \times \dots \times \mathbb{S}^{p+r}$  and  $(N_1, \dots, N_n) \in \mathbb{S}^{p+r} \times \dots \times \mathbb{S}^{p+r}$  such that both  $(M_1, \dots, M_n)$  and  $(N_1, \dots, N_n)$  are in the constraint set  $\Psi$ . Then,  $\Psi$  is a convex set if, and only if, for any  $t \in [0, 1]$ , the linear combination  $(E_1, \dots, E_n) := t(M_1, \dots, M_n) + (1-t)(N_1, \dots, N_n) = (tM_1 + (1-t)N_1, \dots, tM_n + (1-t)N_n) \in \Psi$ . Since  $\Sigma \succeq M_1 \succeq O$  and  $\Sigma \succeq N_1 \succeq O$ , we have  $\Sigma \succeq tM_1 + (1-t)N_1 \succeq O$  and  $E_1 = tM_1 + (1-t)N_1 \in \Psi_1(O)$ . Suppose that  $E_j \in \Psi_j(E_{j-1})$  for  $j = 1, \dots, k-1$ . Since  $\Sigma \succeq M_k \succeq AM_{k-1}A'$ ,  $\Sigma \succeq N_k \succeq AN_{k-1}A'$ , and  $E_{k-1} = tM_{k-1} + (1-t)N_{k-1}$ , we obtain  $\Sigma \succeq tM_k + (1-t)N_k \succeq A'E_{k-1}A'$ , and  $E_k = tM_k + (1-t)N_k \in \Psi_k(E_{k-1})$ . By induction, we conclude that the convex combination  $E \in \Psi$  and therefore  $\Psi$  is a convex set. Note that since the objective function in (9) is linear in  $S_1, \dots, S_n$  (not a zero function) and the constraint set is a non-empty compact (as shown in Proposition 2) and convex set, the global minimum is attained at the *extreme points* of  $\Psi$ .<sup>3</sup>

Next, we formulate the extreme points of  $\Psi$ . To this end, for given  $S_{-k} := \{S_1, \dots, S_{k-1}, S_{k+1}, \dots, S_n\}$ , we introduce the sub-constraint set:

$$\Phi_k(S_{-k}) := \{S_k \in \mathbb{S}^{p+r} \mid \Sigma \succeq S_k \succeq AS_{k-1}A' \wedge A^{-1}S_{k+1}(A')^{-1} \succeq S_k \succeq AS_{k-1}A'\}, \quad (15)$$

<sup>3</sup> An extreme point of a convex set cannot be written as a convex combination of any other points in the set.

for each  $k = 1, \dots, n$ , where we set  $S_0 = O$  and  $S_{n+1} = \Sigma$ . We consider that the sub-constraint set  $\Phi_k(S_{-k}) = \emptyset$  is empty if  $\Sigma - AS_{k-1}A'$  or  $A^{-1}S_{k+1}(A')^{-1} - AS_{k-1}A'$  are not positive semi-definite. Then, the following lemma provides a necessary condition for the extreme points of  $\Psi$  in terms of these sub-constraint sets (15).

**Lemma 4** *If an  $n$ -tuple  $(E_1, \dots, E_n) \in \Psi$  is an extreme point of  $\Psi$ , then for each  $k = 1, \dots, n$ ,  $E_k \in \Phi_k(E_{-k})$  is an extreme point of  $\Phi_k(E_{-k})$ .*

**PROOF.** Suppose that  $E = (E_1, \dots, E_n) \in \Psi$  is an extreme point of  $\Psi$  and there exists an element  $E_k$  such that  $E_k$  is not an extreme point of  $\Phi_k(E_{-k})$ . Then, there exist two distinct  $M, N \in \Phi_k(E_{-k})$  such that  $E_k = tM + (1-t)N$ , for some  $t \in (0, 1)$ . Note that since  $M, N \in \Phi_k(E_{-k})$ , the matrices  $M$  and  $N$  satisfy  $A^{-1}E_{k+1}(A')^{-1} \succeq M \succeq AE_{k-1}A'$  and  $A^{-1}E_{k+1}(A')^{-1} \succeq N \succeq AE_{k-1}A'$  by (15). Therefore, the following  $n$ -tuples

$$E_M := (E_1, \dots, E_{k-1}, M, E_{k+1}, \dots, E_n) \in \Psi$$

$$E_N := (E_1, \dots, E_{k-1}, N, E_{k+1}, \dots, E_n) \in \Psi,$$

and  $E_M \neq E_N$  since  $M \neq N$ . However, we can write the extreme point  $E$  as  $E = tE_M + (1-t)E_N$ , for some  $t \in (0, 1)$  even though  $E_M, E_N \in \Psi$ , and this leads to a contradiction. Hence, if  $(E_1, \dots, E_n) \in \Psi$  is an extreme point, the elements  $E_k$  are the extreme points of the corresponding sub-constraint sets  $\Phi_k(E_{-k})$ .  $\blacksquare$

Now, we seek to formulate the extreme points through the necessary conditions provided in Lemma 4. Let  $(S_1^*, \dots, S_n^*) \in \Psi$  be an extreme point of  $\Psi$ . Then, the element  $S_n^*$  should be an extreme point of  $\Phi_n(S_{-n}^*)$ . To this end, consider arbitrary  $S_1, \dots, S_n$ . Then, in stage- $n$ , the sub-constraint set  $\Phi_n(S_{-n})$  is given by

$$\Phi_n(S_{-n}) = \{S_n \in \mathbb{S}^{p+r} \mid \Sigma \succeq S_n \succeq AS_{n-1}A'\}$$

since we set  $S_{n+1} = \Sigma$  and  $A^{-1}\Sigma(A')^{-1} \succeq \Sigma$ . In order to calculate the extreme point of  $\Phi_n(E_{-n})$ , we use the following proposition.

**Proposition 5** *Under a bijective affine transformation of a convex set, the extreme points are mapped to the extreme points of the transformed set.*

**PROOF.** The proof is provided in the Appendix A.

We note that for each  $k = 1, \dots, n$  if  $\Sigma \succeq S_k$ , then the matrix  $\Sigma - AS_kA'$  is positive definite because  $\Sigma - AS_kA' = A\Sigma A' + Z - AS_kA' = A(\Sigma - S_k)A' + Z$  where  $Z := \mathbb{E}\{z_k z_k'\} = \begin{bmatrix} \Sigma_w & \\ & \Sigma_v \end{bmatrix} \succ O$  and  $\Sigma = A\Sigma A' + Z$  due to the stationarity of

the state and the bias processes. Then, if  $\Sigma \succeq S_{n-1}$ , we have  $\Sigma \succ AS_{n-1}A'$  and the following transformation:

$$F_n(S_n) := (\Sigma - AS_{n-1}A')^{-1/2}(S_n - AS_{n-1}A') \times (\Sigma - AS_{n-1}A')^{-1/2}$$

such that  $F_n$  maps the sub-constraint set  $\Phi_n(S_{-n})$  to

$$F_n(\Phi_n(S_{-n})) = \{P \in \mathbb{S}^{p+r} | I \succeq P \succeq O\}.$$

The following lemma provides the extreme points of the convex set  $\Phi := \{P \in \mathbb{S}^{p+r} | I \succeq P \succeq O\}$ .

**Lemma 6** *A point  $P_e$  in  $\Phi$  is an extreme point if, and only if,  $P_e$  is a symmetric idempotent matrix.*

**PROOF.** The proof is provided in the Appendix B.

Since  $F_n(\cdot)$  is a bijective affine transformation,  $P_o \in \Phi$  is an extreme point of  $\Phi$  if, and only if,  $F_n^{-1}(P_o) \in \Phi_n(S_{-n})$  is an extreme point of  $\Phi_n(S_{-n})$ . Therefore, if  $\Sigma \succeq S_{n-1}$ , the extreme points of  $\Phi_n(S_{-n})$  are given by

$$S_n^* = AS_{n-1}A' + (\Sigma - AS_{n-1}A')^{1/2}P_n(\Sigma - AS_{n-1}A')^{1/2},$$

where  $P_n$  is a symmetric idempotent matrix.

For stage- $(n-1)$ , we have the sub-constraint set:

$$\Phi_{n-1}(S_{-(n-1)}) = \{S_{n-1} \in \mathbb{S}^{p+r} | \Sigma \succeq S_{n-1} \succeq AS_{n-2}A' \wedge A^{-1}S_n(A')^{-1} \succeq S_{n-1} \succeq AS_{n-2}A'\}.$$

We point out that if  $S_{n-1} \in \Phi_{n-1}(S_{-(n-1)})$ , we have  $\Sigma \succeq S_{n-1}$ . Then, setting  $S_n = S_n^*$ , we obtain

$$\Phi_{n-1}(S_{-(n-1)}) = \{S_{n-1} \in \mathbb{S}^{p+r} | \Sigma \succeq S_{n-1} \succeq AS_{n-2}A' \wedge S_{n-1} + \Delta \succeq S_{n-1} \succeq AS_{n-2}A'\},$$

where

$$\Delta := A^{-1}(\Sigma - AS_{n-1}A')^{1/2}P_n(\Sigma - AS_{n-1}A')^{1/2}(A')^{-1} \succeq O.$$

Therefore, if  $S_n$  is an extreme point of  $\Phi_n(S_{-n})$ , the sub-constraint set can be written as

$$\Phi_{n-1}(S_{-(n-1)}) = \{S_{n-1} \in \mathbb{S}^{p+r} | \Sigma \succeq S_{n-1} \succeq AS_{n-2}A'\}.$$

Correspondingly, if  $\Sigma \succeq S_{n-2}$ , the extreme points of  $\Phi_{n-1}(S_{-(n-1)})$  are given by

$$S_{n-1}^* = AS_{n-2}A' + (\Sigma - AS_{n-2}A')^{1/2}P_{n-1}(\Sigma - AS_{n-2}A')^{1/2},$$

where  $P_{n-1}$  is also a symmetric idempotent matrix. Since  $\Sigma \succeq S_{n-1}^*$ , setting  $S_{n-1} = S_{n-1}^*$ , we have

$$S_n^* = AS_{n-1}^*A' + (\Sigma - AS_{n-1}^*A')^{1/2}P_n(\Sigma - AS_{n-1}^*A')^{1/2}.$$

Following identical steps, we obtain that any extreme point  $(S_1^*, \dots, S_n^*)$  of  $\Psi$  should satisfy (14).  $\square$

In the next section, we address the tightness of the bound (9), i.e., whether the lower bound can be achieved through certain sender policies or not.

## 5 Equilibrium Achieving Policies

Even though Theorem 3 characterizes necessary and sufficient conditions for the minimizing arguments of the SDP problem (9), it still does not provide the solutions explicitly. However, as we will show next, these results have important consequences in the characterization of equilibrium achieving strategies within the general class of policies. In particular, sender strategies that can be constructed to yield posterior covariances in (14) can minimize the lower bound (9), and therefore can minimize the main objective function (8).

The following theorem says that for any solutions of (9), say  $S_1^*, \dots, S_n^*$ , there exist certain deterministic matrices  $B_k \in \mathbb{R}^{(p+r) \times (p+r)}$  for  $k = 1, \dots, n$ , such that the memoryless linear disclosure policies

$$\eta_k(\mathbf{x}_k, \boldsymbol{\theta}_k) = B_k' \mathbf{s}_k, \quad (16)$$

result in the posterior covariance matrices  $R_1 = S_1^*, \dots, R_n = S_n^*$ . In particular, by minimizing the lower bound on  $S$ 's objective function, the memoryless linear sender policies (16) yield the multi-stage Stackelberg equilibrium within the general class of policies.

**Theorem 7** *Let  $S_1^*, \dots, S_n^*$  be the solutions of the SDP problem (9) and  $P_1, \dots, P_k$  be the corresponding symmetric idempotent matrices in (14). Let  $P_k$ ,  $k = 1, \dots, n$ , have the eigen decompositions:  $P_k = U_k \Lambda_k U_k'$ . Then, for  $B_k = (\Sigma - AS_{k-1}^*A')^{-1/2}U_k \Lambda_k$ , memoryless linear sender strategies (16) yield the multi-stage equilibrium (8) within the general class of policies.*

**PROOF.** Consider that  $S$  employs memoryless linear policies as in (16) for some deterministic combination matrices  $B_1, \dots, B_n \in \mathbb{R}^{p+r}$ . Correspondingly, the first moments of the posteriors, for  $k = 1, \dots, n$ , are given by  $\hat{\mathbf{s}}_k = \mathbb{E}\{\mathbf{s}_k | \mathbf{y}_{[1,k]}\} = \mathbb{E}\{\mathbf{s}_k | B_1 \mathbf{s}_1, \dots, B_k \mathbf{s}_k\}$ . At stage-1, we have

$$\begin{aligned} \mathbb{E}\{\mathbf{s}_1 | \mathbf{y}_1\} &= \mathbb{E}\{\mathbf{s}_1 \mathbf{y}_1'\} \mathbb{E}\{\mathbf{y}_1 \mathbf{y}_1'\}^{-1} \mathbf{y}_1 \\ &= \mathbb{E}\{\mathbf{s}_1 \mathbf{s}_1'\} B_1 (B_1' \mathbb{E}\{\mathbf{s}_1 \mathbf{s}_1'\} B_1)^{-1} B_1' \mathbf{s}_1 \\ &= \Sigma B_1 (B_1' \Sigma B_1)^{-1} B_1' \mathbf{s}_1. \end{aligned} \quad (17)$$

Here, we take the pseudo-inverse of  $B_1' \Sigma B_1$  since it can be singular if  $B_1$  has a rank smaller than  $p + r$ . For example,  $\Sigma$  can disclose  $\eta_k(\mathbf{x}_k, \boldsymbol{\theta}_k) = [\mathbf{x}_k' \ 0']'$ , i.e., a rank  $p$  matrix  $B_1 = \begin{bmatrix} I & O \\ O & O \end{bmatrix}$ , where  $I$  is of dimension  $p \times p$  and  $O$ 's have the corresponding dimensions.

In order to calculate  $\hat{\mathbf{s}}_2$ , we first consider the following covariance matrix:

$$\begin{aligned} & \mathbb{E}\{(\mathbf{s}_2 - \mathbb{E}\{\mathbf{s}_2|\mathbf{y}_1\})(\mathbf{s}_2 - \mathbb{E}\{\mathbf{s}_2|\mathbf{y}_1\})'\} \\ &= \mathbb{E}\{(\mathbf{A}\mathbf{s}_1 + \mathbf{z}_1 - \mathbf{A}\hat{\mathbf{s}}_1)(\mathbf{A}\mathbf{s}_1 + \mathbf{z}_1 - \mathbf{A}\hat{\mathbf{s}}_1)'\}, \end{aligned}$$

where  $\mathbb{E}\{\mathbf{s}_2|\mathbf{y}_1\} = \mathbf{A}\hat{\mathbf{s}}_1$  as shown in (11). Since  $\mathbf{z}_1$  is independent of  $\mathbf{y}_1$ , the noise term  $\mathbf{z}_1$  is also independent of  $\mathbb{E}\{\mathbf{s}_1|\mathbf{y}_1\}$ . Then, we obtain

$$\begin{aligned} & \mathbb{E}\{(\mathbf{A}\mathbf{s}_1 + \mathbf{z}_1 - \mathbf{A}\hat{\mathbf{s}}_1)(\mathbf{A}\mathbf{s}_1 + \mathbf{z}_1 - \mathbf{A}\hat{\mathbf{s}}_1)'\} \\ &= \mathbf{A}\mathbb{E}\{(\mathbf{s}_1 - \hat{\mathbf{s}}_1)(\mathbf{s}_1 - \hat{\mathbf{s}}_1)'\} \mathbf{A}' + \mathbf{Z}, \\ &\stackrel{(a)}{=} \mathbf{A}(\Sigma - \mathbf{R}_1)\mathbf{A}' + \mathbf{Z}, \\ &\stackrel{(b)}{=} \Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}', \end{aligned} \quad (18)$$

where (a) is due to (10), and (b) holds since  $\mathbf{A}\Sigma\mathbf{A}' + \mathbf{Z} = \Sigma$  due to the stationarity of the state and the bias processes. Correspondingly, by (18) and the linear policy  $\mathbf{y}_2 = \mathbf{B}_2'\mathbf{s}_2$ , the conditional first moment of the second-stage action  $\mathbf{y}_2$  is given by  $\mathbb{E}\{\mathbf{y}_2|\mathbf{y}_1 = y_1\} = \mathbf{B}_2'\mathbb{E}\{\mathbf{s}_2|\mathbf{y}_1 = y_1\}$ . We have the cross correlation:

$$\mathbb{E}\{(\mathbf{y}_2 - \mathbb{E}\{\mathbf{y}_2|\mathbf{y}_1\})(\mathbf{s}_2 - \mathbb{E}\{\mathbf{s}_2|\mathbf{y}_1\})'\} = \mathbf{B}_2'(\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}'), \quad (19)$$

and the conditional covariance of  $\mathbf{y}_2$  is given by

$$\mathbb{E}\{(\mathbf{y}_2 - \mathbb{E}\{\mathbf{y}_2|\mathbf{y}_1\})(\mathbf{y}_2 - \mathbb{E}\{\mathbf{y}_2|\mathbf{y}_1\})'\} = \mathbf{B}_2'(\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2. \quad (20)$$

Due to the linear sender policies, the disclosed information is also Gaussian. By (18), (19), and (20), the joint distribution of  $\mathbf{s}_2$  and the second stage action  $\mathbf{y}_2$  conditioned on the first stage action  $\mathbf{y}_1 = y_1$  is given by

$$\begin{bmatrix} \mathbf{s}_2 \\ \mathbf{y}_2 \end{bmatrix} \Big| \mathbf{y}_1 = y_1 \sim \mathbb{N} \left( \begin{bmatrix} \mathbf{A}\hat{\mathbf{s}}_1 \\ \mathbf{B}_2'\mathbf{A}\hat{\mathbf{s}}_1 \end{bmatrix}, \begin{bmatrix} \Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}' & (\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2 \\ \mathbf{B}_2'(\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}') & \mathbf{B}_2'(\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2 \end{bmatrix} \right).$$

The first order conditional moment is given by

$$\begin{aligned} \mathbb{E}\{\mathbf{s}_2|\mathbf{y}_1 = y_1, \mathbf{y}_2 = y_2\} &= \mathbf{A}\hat{\mathbf{s}}_1 + (\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2 \\ &\quad \times (\mathbf{B}_2'(\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2)^+ (\mathbf{y}_2 - \mathbf{B}_2'\mathbf{A}\hat{\mathbf{s}}_1) \end{aligned}$$

and correspondingly, we obtain

$$\hat{\mathbf{s}}_2 = \mathbf{A}\hat{\mathbf{s}}_1 + (\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2(\mathbf{B}_2'(\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2)^+ \mathbf{B}_2'(\mathbf{s}_2 - \mathbf{A}\hat{\mathbf{s}}_1) \quad (21)$$

almost everywhere. As we derived (21), for  $k > 2$ , the first moments of the posteriors can be written as

$$\hat{\mathbf{s}}_k = (\Sigma - \mathbf{A}\mathbf{R}_{k-1}\mathbf{A}')\mathbf{B}_k(\mathbf{B}_k'(\Sigma - \mathbf{A}\mathbf{R}_{k-1}\mathbf{A}')\mathbf{B}_k)^+ \mathbf{B}_k'(\mathbf{s}_k - \mathbf{A}\hat{\mathbf{s}}_{k-1}) + \mathbf{A}\hat{\mathbf{s}}_{k-1}.$$

Next, we seek to calculate  $\mathbf{R}_k = \mathbb{E}\{\hat{\mathbf{s}}_k\hat{\mathbf{s}}_k'\}$ , for  $k = 1, \dots, n$ . By (17), we obtain

$$\begin{aligned} \mathbf{R}_1 &= \Sigma \mathbf{B}_1(\mathbf{B}_1'\Sigma\mathbf{B}_1)^+ \mathbf{B}_1' \mathbb{E}\{\mathbf{s}_1\mathbf{s}_1'\} \mathbf{B}_1(\mathbf{B}_1'\Sigma\mathbf{B}_1)^+ \mathbf{B}_1'\Sigma \\ &= \Sigma \mathbf{B}_1(\mathbf{B}_1'\Sigma\mathbf{B}_1)^+ \mathbf{B}_1'\Sigma \end{aligned}$$

since  $\mathbb{E}\{\mathbf{s}_1\mathbf{s}_1'\} = \Sigma$ , and for a matrix  $M$  and its pseudo-inverse  $M^+$ ,  $M^+MM^+ = M$ . By (21), in  $\mathbf{R}_2$ , we have a cross-term  $\mathbb{E}\{\hat{\mathbf{s}}_1(\mathbf{s}_2 - \mathbf{A}\hat{\mathbf{s}}_1)'\}$ , which can be written as

$$\begin{aligned} \mathbb{E}\{\hat{\mathbf{s}}_1(\mathbf{s}_2 - \mathbf{A}\hat{\mathbf{s}}_1)'\} &= \mathbb{E}\{\hat{\mathbf{s}}_1\mathbf{s}_2'\} - \mathbb{E}\{\hat{\mathbf{s}}_1\hat{\mathbf{s}}_1'\}\mathbf{A}' \\ &\stackrel{(a)}{=} \mathbf{R}_1\mathbf{A}' - \mathbf{R}_1\mathbf{A}' = \mathbf{O}, \end{aligned} \quad (22)$$

where (a) is due to the law of iterated expectations and by (11) such that  $\mathbb{E}\{\hat{\mathbf{s}}_1\mathbf{s}_2'\} = \mathbb{E}\{\mathbb{E}\{\hat{\mathbf{s}}_1\mathbf{s}_2'|\mathbf{y}_1\}\} = \mathbb{E}\{\hat{\mathbf{s}}_1\mathbb{E}\{\mathbf{s}_2'|\mathbf{y}_1\}\} = \mathbb{E}\{\hat{\mathbf{s}}_1\hat{\mathbf{s}}_1'\}\mathbf{A}'$ . Then, (18), (19), (21), and (22) lead to

$$\begin{aligned} \mathbf{R}_2 &= \mathbf{A}\mathbf{R}_1\mathbf{A}' + (\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2 \\ &\quad \times \underbrace{(\mathbf{B}_2'(\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2)^+ \mathbf{B}_2'(\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2(\mathbf{B}_2'(\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2)^+}_{(\mathbf{B}_2'(\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2)^+} \\ &\quad \times \mathbf{B}_2'(\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}') \\ &= \mathbf{A}\mathbf{R}_1\mathbf{A}' + (\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2(\mathbf{B}_2'(\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}')\mathbf{B}_2)^+ \mathbf{B}_2'(\Sigma - \mathbf{A}\mathbf{R}_1\mathbf{A}'). \end{aligned}$$

Correspondingly, for  $k > 2$ , we have

$$\mathbf{R}_k = (\Sigma - \mathbf{A}\mathbf{R}_{k-1}\mathbf{A}')\mathbf{B}_k(\mathbf{B}_k'(\Sigma - \mathbf{A}\mathbf{R}_{k-1}\mathbf{A}')\mathbf{B}_k)^+ \mathbf{B}_k'(\Sigma - \mathbf{A}\mathbf{R}_{k-1}\mathbf{A}') + \mathbf{A}\mathbf{R}_{k-1}\mathbf{A}'.$$

Let  $\mathbf{C}_1 := \Sigma^{1/2}\mathbf{B}_1$  and  $\mathbf{C}_k := (\Sigma - \mathbf{A}\mathbf{R}_{k-1}\mathbf{A}')^{1/2}\mathbf{B}_k$  for  $k = 2, \dots, n$  such that

$$\begin{aligned} \mathbf{R}_1 &= \Sigma^{1/2}\mathbf{C}_1(\mathbf{C}_1'\mathbf{C}_1)^+ \mathbf{C}_1'\Sigma^{1/2} \\ \mathbf{R}_k &= (\Sigma - \mathbf{A}\mathbf{R}_{k-1}\mathbf{A}')^{1/2}\mathbf{C}_k(\mathbf{C}_k'\mathbf{C}_k)^+ \mathbf{C}_k'(\Sigma - \mathbf{A}\mathbf{R}_{k-1}\mathbf{A}')^{1/2} \\ &\quad + \mathbf{A}\mathbf{R}_{k-1}\mathbf{A}'. \end{aligned}$$

Note that  $\mathbf{C}_k(\mathbf{C}_k'\mathbf{C}_k)^+ \mathbf{C}_k'$ , for  $k = 1, \dots, n$ , is a symmetric idempotent matrix and the posterior covariances  $\mathbf{R}_1, \dots, \mathbf{R}_n$  have identical expressions as in (14). If the symmetric idempotent matrices  $\mathbf{P}_k$  for  $k = 1, \dots, n$  corresponding to the minimizers of the SDP problem (9) have the eigen decompositions:  $\mathbf{P}_k = \mathbf{U}_k\boldsymbol{\Lambda}_k\mathbf{U}_k'$ , we can set  $\mathbf{C}_k = \mathbf{U}_k\boldsymbol{\Lambda}_k$  for  $k = 1, \dots, n$  such that  $\mathbf{C}_k(\mathbf{C}_k'\mathbf{C}_k)^+ \mathbf{C}_k' = \mathbf{P}_k$ . In particular, setting  $\mathbf{B}_1 = \Sigma^{-1/2}\mathbf{U}_1\boldsymbol{\Lambda}_1$  and  $\mathbf{B}_k = (\Sigma - \mathbf{A}\mathbf{S}_{k-1}^*\mathbf{A}')^{-1/2}\mathbf{U}_k\boldsymbol{\Lambda}_k$ , we obtain  $\mathbf{R}_k = \mathbf{S}_k^*$  for  $k = 1 \dots n$ . Hence, the memoryless linear



disclosure policies can minimize the main objective function (8) within the general class of policies.  $\square$

**Remark 8** *We point out that existence of equilibrium achieving strategies is not guaranteed within the general class of policies. Therefore, by formulating equilibrium achieving policies, we also show the existence of equilibrium in the hierarchical multi-stage Gaussian signaling game.*

*For linear sender strategies, the corresponding equilibrium achieving receiver strategies are also linear since the underlying states are jointly Gaussian.*

*In addition to the memoryless linear sender strategies in Theorem 7, any bijective transformation of these policies also results in the same posteriors and can yield the equilibrium.*

*We point out that in general, the equilibrium achieving sender strategy  $\eta_k$  is not a linear function of solely the innovations in the state processes, i.e.,  $\mathbf{x}_k - \mathbb{E}\{\mathbf{x}_k | \mathbf{x}_{[1,k-1]}\}$  and  $\boldsymbol{\theta}_k - \mathbb{E}\{\boldsymbol{\theta}_k | \boldsymbol{\theta}_{[1,k-1]}\}$ , due to the asymmetric information paradigm.*

## 6 Conclusion

In this paper, we have addressed the existence and characterization of the equilibrium achieving sender strategies in hierarchical signaling games with finite horizon for quadratic objective functions and multi-variate Gaussian processes. Our main conclusion has been that memoryless linear sender strategies can yield the equilibrium in this dynamic game within the general class of policies. This addresses an open question on the structure of equilibrium achieving policies in dynamic strategic information transmission.

Some future directions of research on this topic include characterization of equilibrium achieving strategies when there is a channel between the agents, and strategic design of measurement and control strategies for stochastic systems with feedback, as an extension of [4] to the strategic settings.

## Acknowledgements

This research was supported in part by the U.S. Office of Naval Research (ONR) MURI grant N00014-16-1-2710, and in part by NSF under grant CCF 11-11342.

## References

- [1] E. Akyol, C. Langbort, and T. Başar. Privacy constrained information processing. In *Proc. of 54th IEEE Conf. Decision and Control, CDC, Japan*, pages 4511–4516, 2015.
- [2] E. Akyol, C. Langbort, and T. Başar. Information-theoretic approach to strategic communication as a hierarchical game. *Proceedings of the IEEE*, 2017. in press.
- [3] T. Başar and G. Olsder. *Dynamic Noncooperative Game Theory*. Society for Industrial Mathematics (SIAM) Series in Classics in Applied Mathematics, 1999.
- [4] R. Bansal and T. Başar. Simultaneous design of measurement and control strategies for stochastic systems with feedback. *Automatica*, 25(5):679–694, 1989.
- [5] V. Crawford and J. Sobel. Strategic information transmission. *Econometrica: Journal of the Econometric Society*, pages 1431–1451, 1982.
- [6] F. Farokhi, A. Teixeira, and C. Langbort. Estimation with strategic sensors. *IEEE Transactions on Automatic Control*. in press.
- [7] M. Gentzkow and E. Kamenica. Bayesian persuasion. *American Economic Review*, 101(6):2590–2615, 2011.
- [8] I. Greenberg. The effect of deception on optimal decisions. *Operations Research Letters*, 4, 1982.
- [9] I. Greenberg. The role of deception in decision theory. *Journal of Conflict Resolution*, 26:139–156, 1982.
- [10] Y. Han, J. Chan, T. Alpcan, and C. Leckie. Using virtual machine allocation policies to defend against co-resident attacks in cloud computing. *IEEE Trans. Dependable and Secure Computing*, 2015. in press.
- [11] Y. Han, J. Chan, T. Alpcan, C. Leckie, and B. I. P. Rubinstein. A game theoretical approach to defend against co-resident attacks in cloud computing: Preventing co-residence using semi-supervised learning. *IEEE Trans. Information Forensics and Security*, 11(3):556–570, 2015.
- [12] A. Kashyap, T. Başar, and R. Srikant. Quantized consensus. *Automatica*, 43(7):1192–1203, 2007.
- [13] D. Li and J. B. Cruz-Jr. Information, decision-making and deception in games. *Decision Support Systems*, 47:518–527, 2009.
- [14] S. Saritas, S. Yüksel, and S. Gezici. Dynamic signaling games under Nash and Stackelberg equilibria. In *Proc. IEEE International Symposium on Information Theory*, 2016.
- [15] M. O. Sayin, E. Akyol, and T. Başar. On the structure of equilibrium strategies in dynamic Gaussian signaling games. In *Proc. 2016 IEEE Multi-Conference on Systems and Control (MSC)*, Buenos Aires, Argentina, 2016.
- [16] M. O. Sayin, E. Akyol, and T. Başar. Strategic control of a tracking system. In *Proc. 55th IEEE Conf. Decision and Control, CDC, Las Vegas, Nevada*, 2016.
- [17] W. Tamura. A theory of multidimensional information disclosure. *Working paper, available at SSRN 1987877*, 2014.
- [18] Q. Zhu and T. Başar. Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems. *IEEE Control Systems*, 35(1):46–65, 2015.

## A Proof of Proposition 5

Consider a bijective affine transformation  $F(\cdot)$  of a convex set  $\Pi$ . Since  $\Pi$  is a convex set, for any point in  $\Pi$ , say  $Z$ , there exist points  $M, N \in \Pi$  such that  $Z = tM + (1-t)N$  for any  $t \in [0, 1]$ . Then, under affine transformation, this relation is preserved since  $F(Z) = F(tM + (1-t)N) = tF(M) + (1-t)F(N)$ . Therefore, the transformed set  $F(\Pi)$  is also convex.

If  $Z \in \Pi$  is not an extreme point, then there exist distinct points  $M, N \in \Pi$  such that  $Z = tM + (1-t)N$  for some  $t \in (0, 1)$ . The transformation  $F(z)$  can be written as  $F(Z) = tF(M) + (1-t)F(N)$  for some  $t \in (0, 1)$  and therefore  $F(Z)$

is not an extreme point of  $F(\Pi)$ . Correspondingly,  $F^{-1}(\cdot)$  is a bijective affine mapping of the convex set  $F(\Pi)$ , and if  $Z_o \in F(\Pi)$  is not an extreme point, then  $F^{-1}(Z_o) \in \Pi$  is not an extreme point of  $\Pi$ . Therefore,  $Z$  is not an extreme point of  $\Pi$  if, and only if,  $F(Z)$  is not an extreme point of  $F(\Pi)$ .

## B Proof of Lemma 6

Suppose that for an idempotent matrix  $P \in \Phi$ , there exist two distinct matrices  $M \in \Phi$  and  $N \in \Phi$  such that  $P = tM + (1-t)N$  for some  $t \in (0, 1)$ . Let  $p_1, p_0 \in \mathbb{R}^{p+r}$  be eigenvectors of  $P$  corresponding to eigenvalues 1 and 0, respectively. Note that since the eigenvalues of  $M$  and  $N$  are bounded, for any vector  $p \in \mathbb{R}^{p+r}$ ,  $0 \leq p'Mp \leq 1$  and  $0 \leq p'Np \leq 1$ . Then, through convex combination, we have

$$\begin{aligned} tp'_1Mp_1 + (1-t)p'_1Np_1 &= p'_1Pp_1 = 1 \\ tp'_0Mp_0 + (1-t)p'_0Np_0 &= p'_0Pp_0 = 0, \end{aligned}$$

which leads to  $p'_1Mp_1 = p'_1Np_1 = 1$  and  $p'_0Mp_0 = p'_0Np_0 = 0$ . Therefore,  $p_1$  and  $p_0$  are eigenvectors of  $M$  and  $N$ . Furthermore, the eigenvalues of  $M$  and  $N$  corresponding to the eigenvectors  $p_1$  and  $p_0$  are 1 and 0, respectively. Since  $p_1$  and  $p_0$  are arbitrary eigenvectors of  $P$ , the matrices  $M$  and  $N$  have the same eigenvalues and eigenvectors with  $P$  and correspondingly  $P = M = N$ , which, however, yields a contradiction. In view of these contradictions, we can say that a symmetric idempotent matrix is an extreme point of  $\Phi$ .

Lastly, we aim to show that any other matrix which is not an idempotent matrix, say  $Z$ , cannot be an extreme point of  $\Phi$ . Let  $Z$  have an eigen-decomposition

$$Z = Q \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_{p+r} \end{bmatrix} Q'.$$

Since  $Z$  is not an idempotent matrix, there exists an eigenvalue, say  $\lambda_i$ , which is neither 1 nor 0. Then, for any  $t \in (0, 1)$ , there exist two distinct  $\lambda_{i,1}, \lambda_{i,2} \in [0, 1]$  such that  $\lambda_i = t\lambda_{i,1} + (1-t)\lambda_{i,2}$ , e.g., set  $\lambda_{i,1} = \lambda_i/t$  and  $\lambda_{i,2} = 0$ . Correspondingly, for the matrices:

$$M := Q \begin{bmatrix} \ddots & & \\ & \lambda_{i,1} & \\ & & \ddots \end{bmatrix} Q', \quad N := Q \begin{bmatrix} \ddots & & \\ & \lambda_{i,2} & \\ & & \ddots \end{bmatrix} Q',$$

we have  $Z = tM + (1-t)N$ , yet  $M \neq N$ , i.e.,  $Z$  is not an extreme point of  $\Phi$ .